Applicant : Christopher A. Rygaard   Attorney's Docket No.: 18511-007001
Serial No. : 09/764,548
Filed   : January 18, 2001
Page   : 8 of 12

REMARKS

The subject application is currently under appeal due to the Notice of Appeal filed on October 7, 2004. In conjunction with a Request for Continuing Examination accompanying this Reply, Applicant submits the following remarks in reply to the Final Office Action of April 7, 2004. The Office Action rejected claims 1-21. Applicant thanks Examiner for examination.

In response, the specification has been amended as indicated above. Claims have been canceled as indicated above. Claims have been added as indicated above. No new matter has been added. Applicant respectfully requests reconsideration in view of the foregoing amendments and these remarks.

Rejections to the Claims under 35 U.S.C. § 102(b)

The Official Action rejected claims 1-21 under 35 U.S.C. § 102(b) as being anticipated by *NIST Special Publication 800-19 – Mobile Agent Security* by Jansen ("Jansen"). In addition, the Official Action indicated that the claims could likewise be anticipated by *Jumping Beans White Paper* by Ad Astra Eng., Inc. ("the White Paper"). Applicant respectfully submits that the new claims traverse the rejections.

<u>Claim 22</u>

New independent claim 22 recites a system including a first module, a second module, and a third module. The first module stores first content data related to a mobile application. The first data content is stored prior to a jump to a receiving host. The second module receives second content data related to the mobile application. The second content data is received from a receiving host prior to instantiation of the mobile application. The fourth module detects unwanted changes including comparing the first and second content data.

Jansen generally discloses a survey of security issues associated with mobile software agent technology. Jansen discloses that an agent system addresses some security issues by implementing a client-server architecture. (p. 18-19). Jansen discloses a reference monitor to ensure that agents on a platform are not able to interfere with each other or with the platform. (p.

13). To do so, the reference monitor establishes separate isolated domains for each agent and the platform, and controls all inter-domain access. (p. 14) The reference manager is always invoked and is non-bypassable. (Id.). Jansen discloses that an agent can modify another agent on a platform if the platform has no control mechanisms in place. (p. 5). Jansen also discloses that a platform modification of an agent can be detected by having an original author digitally sign agent code. (p. 6-7). Finally, Jansen discloses an agent itinerary that can be tracked and recorded by a cooperating agent. (p. 21).

However, Jansen fails to teach or suggest every limitation of claim 22. Specifically, Jansen fails to teach "*a first module to store, prior to a jump to the receiving host, first content data associated with the mobile application.*" Foremost, Jansen only discloses a client-server architecture to address security issues in the abstract, and without proposing how to address the security issues with specific techniques occurring at a server. Furthermore, the reference monitor cited in the Official Action is directed to a control mechanism *on a platform* on which the agent executes for protecting one agent from another agent. Jansen fails to disclose functional advantages associated with a central architecture of a centralized security enforcement node that is separated from potential hostilities associated with a receiving host, a dispatching host, and a mobile application. The claimed first module, disposed on the centralized security enforcement node, avoids intermixing with potential hostilities. Thus, Jansen fails to teach or suggest the first module of claim 22.

Jansen also fails to teach "*a second module to receive from the receiving host, prior to instantiation of the mobile application on the receiving host, second content data associated with the mobile application.*" As discussed, Jansen fails to teach or suggest Applicant's claimed centralized techniques. With respect to the decentralized architecture, the agent in Jansen must execute on the platform in order to record or track itineraries after moving to an accepting host. Therefore, Jansen teaches away from Applicant's claimed centralized techniques that include receiving a second content data prior to instantiation. Thus, Jansen fails to disclose the second module of claim 22.

Jansen additionally fails to teach or suggest "*a third module...to detect unwanted changes in contents of the mobile application including comparing the first and second content data.*" As discussed, Jansen fails to teach or suggest Applicant's claimed centralized techniques. With respect to the decentralized architecture discussed above, the agents in Jansen are specifically protecting cooperating agents themselves against a hostile platform. The technique of Jansen is insufficient for protection against hostile cooperating agents. The third module compares the first and second content data and can be used to protect against hostile cooperating agents. Thus, Jansen fails to disclose the third module of claim 22. Thus, Applicant, respectfully submits that claim 22 is patentable over Jansen.

The White Paper referred to above generally discloses a development tool for building mobile applications and associated security issues. The White Paper discloses detecting unwanted behavior primarily through the use of authorization techniques for starting an agency and creating a mobile application. (p. 14). Also, the White Paper discloses a worst-case technique for each hop of a multi-hop scenario and trusts a mobile application only as much as the least trusted agency it has visited. (p. 15). The White Paper does disclose passing a mobile application through a server when moving from one host to another. (p. 9). Similarly, the White Paper also discloses protecting code of the mobile application by rejecting attempts to write a file that could be an attack. (p. 21).

However, the White Paper fails to disclose all of the limitations of claim 22. As to the first module, nowhere does the White Paper disclose storing first content data. The White Paper discloses a centralized architecture in which a server receives a mobile application itself from a dispatching host before moving to another host. The server interception requires that a dispatching host and a receiving host be connected to the server, thwarting the peer-to-peer communication of claim 22. Further, while Applicant's claimed third module compares first and second content data (second content data from the receiving host prior to instantiation of the mobile application), the White Paper is centralized architecture that has no need to receive anything from the receiving host. The White Paper discloses centralized architecture receiving the mobile application itself, and accordingly, does not require receipt of second content data

from the receiving host. As discussed above, the mobile application of claim 22 has yet to be instantiated. Thus, the White Paper fails to disclose the third module of claim 22.

Since the White Paper fails to cure the deficiencies of Jansen, Applicant submits that claim 22 is patentable over a combination of Jansen and the White Paper. Furthermore, new claims depending on independent claim 22 are patentable for at least the same reasons as claim 22.

Claim 29

New independent claim 29 recites a method at a centralized security enforcement node including storing, receiving, and detecting steps. First content data is stored prior to a jump. Second content data is received prior to instantiation of the mobile application. Unwanted changes in contents of the mobile application are detected including comparing the first and second content data. Applicant submits that, for at least the same reasons as discussed with respect to claim 22, claim 29 and related dependent claims are patentable over Jansen and/or the White Paper.

Clam 36

New independent claim 36 recites a computer program product including program instructions tangibly stored on a computer-readable medium and operable to cause a computer system to perform a method at a centralized security enforcement node including storing, receiving, and detecting steps. First content data is stored prior to a jump. Second content data is received prior to instantiation of a mobile application. Unwanted changes in contents of the mobile application are detected including comparing the first and second content data. Applicant submits that, for at least the same reasons as discussed with respect to claim 22, that claim 36 and related dependent claims are patentable over Jansen and/or the White Paper.

Applicant : Christopher A. Rygaard
Serial No. : 09/764,548   Attorney's Docket No.: 18511-007001
Filed   : January 18, 2001
Page   : 12 of 12

Conclusion

Therefore, Applicant respectfully submits that the presented claims are patentable over Jansen and/or the White Paper and are in condition for allowance.
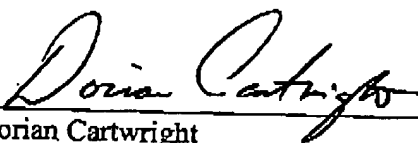
Pursuant to 37 C.F.R. § 1.136, Applicant hereby petitions that the period for response to the action dated December 7, 2004, be extended for two months to and including February 7, 2005. Please charge the extension fee to Deposit Account No. 06-1050.

Please charge any deficiency in fees or credit any over payment to Deposit Account No. 06-1050.

Respectfully submitted,

Date:_____2/7/05_____

Dorian Cartwright
Reg. No. 53,853

Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, California 94063
Telephone: (650) 839-5017
Facsimile: (650) 839-5071

50260081.doc